



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/625,547	07/25/2000	Laurence Hamid	12-52 US	7157

7590

12/01/2005

Gordon Freedman
Freedman & Associates
117 CentrepoinTE Drive
Suite 350
Nepean, ON K2G 5X3
CANADA

EXAMINER

ZAND, KAMBIZ

ART UNIT

PAPER NUMBER

2132

DATE MAILED: 12/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/625,547

Applicant(s)

HAMID ET AL.

Examiner

Kambiz Zand

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 October 2005.
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☒ Claim(s) 1-10 is/are allowed.
6) ☒ Claim(s) 11-20 is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on 14 December 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

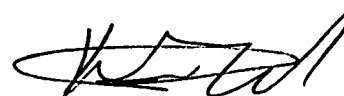
- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____

- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____



DETAILED ACTION

1. The text of those sections of Title 35, U.S. Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. Claims 1, 9, 11 and 14 have been amended.
4. Claims 1-20 are pending.

Response to Arguments

5. Applicant's arguments with respect to claims 9-10 have been persuasive and the rejection of claims 9-10 has been withdrawn.
6. Applicant's arguments with respect to claim 11 filed 10/20/2005 have been fully considered but they are moot in view of the new ground(s) of rejection. Examiner also makes the following remarks: changing a password is being disclosed below, however examiner remain the applicants that if the second password is only the updated or a change from the first password then validity of the first password after the change is questionable and therefore the claim limitation is reduced to just protecting a file having a password where such password keep changing regardless of what it is called (second, master, etc.). Therefore the allowability of the claim 14 has been withdrawn upon such interpretation unless

applicant clear if the first password after being changed still valid and is protecting a file, and the new changed first password is being called a second password for protecting another file. That is the second password is derived from the first password.

7. Examiner has kept the rejection of the claim 11 addressing the change based on the understanding that both the first password, and the changed first password (called second password by applicant) both valid at the same time, protecting two different file or a file if one consider the second password as the master password to get into the first password.
8. Claim 14 allowability has been withdrawn on the understanding that once the first password is changed, it is no longer valid, therefore incorporation of the claim 14 into independent claim 11 only represent accessing a password that is being updated or changed and it is corresponds to a user having different authorization level.

Claim Rejections - 35 USC § 102

9. **Claims 11 and 15-19** are rejected under 35 U.S.C. 102(e) as being anticipated by Nielson (6,182,229 B1).

As per claim 11 Nielson (6,182,229 B1) teach a method of changing a first password for securing files accessible by password data entry comprising the steps of:

Art Unit: 2132

determining a plurality of files secured with the first password (see col.3, line67 and col.4, lines 1-2 where passwords within the database protect the remote server; col.3, lines 12-22 where a table with each entry of URL specifies the site access protocol and the name of the site where each URLs corresponds to plurality of files (please see definition of URL in a computer dictionary), and the encrypted password that corresponding to a url file as depicted in fig.2 corresponds to Applicant's first password that secure the file) ; authorizing a change from the first password to a second other password for securing the plurality of files (see col.19-20 where it disclose the password particular to specific site (URL address (file) could be random (changed or updated) for enhancing the security where such password corresponds to Applicant's first, second or any passwords in the database ;col.3, lines 21-24 disclose a master password that being used to encrypt the passwords for the remote server entry and possibly the ids, this master password corresponds to the second password that protects security for the urls by encrypting the access password of url); for each file secured with the first password, accessing the file with the first password (see fig.2 where the first password corresponds the url is used to access the web site once is decrypted, it also can be done manually or automatically) and securing the file with the second other password (see col.3, lines 21-24 disclose a master password that being used to encrypt the passwords for the remote server entry and possibly the ids, this master password corresponds to the second password that protects security for the urls that corresponds to files that are being secured) ; storing the second other

Art Unit: 2132

password in the password database (**see col.4, lines 34-36 where it disclose the master password that corresponds to Applicant's second password is stored in the memory; fig.3, item 312 and 314 disclose the master password or second password stored in the password database**).

As per claim 15 Nielson (6,182,229 B1) teach the method of changing a first password for securing files accessible by password data entry as defined in claim 11 wherein the step of determining a plurality of files secured with the first password comprises the step of determining from the password database, files associated with the first password (**see col.3, line67 and col.4, lines 1-2 where passwords within the database protect the remote server; col.3, lines 12-22 where a table with each entry of URL specifies the site access protocol and the name of the site where each URLs corresponds to plurality of secure files and the encrypted password corresponding to a url file as depicted in fig.2 corresponds to Applicant's first password**).

As per claim 16 Nielson (6,182,229 B1) teach the method of changing a first password for securing files accessible by password data entry as defined in claim 15 wherein those files associated with the first password are identified because they are identified by an identifier associated with the first password (**see fig.2 where user id associate with their corresponding password and file url; col.3, lines 48-53 where the association with controlled web site or a page. Examiner has considered address**

Art Unit: 21:32

of secure web site URL as a file that need password for access since url address could corresponds to a particular file for access).

As per claim 17 Nielson (6,182,229 B1) teach the method of changing a first password for securing files accessible by password data entry as defined in claim 11 wherein the step of determining a plurality of files secured with the first password comprises the step of determining from accessible files, those files associated with the first password **(see fig.2 where user id associate with their corresponding password and file url; col.3, lines 48-53 where the association with controlled web site or a page.**

Examiner has considered address of secure web site URL as a file that need password for access since url address could corresponds to a particular file for access and they are secure since the password and possibly user IDs are encrypted as depicted in fig.2).

As per claim 18 Nielson (6,182,229 B1) teach the method of changing a first password for securing files accessible by password data entry as defined in claim 11 wherein the step of providing a second other password includes the step of automatically generating the second other password **(see col.5, lines 555-61 where it disclose passwords can be generated automatically by password management).**

As per claim 19 Nielson (6,182,229 B1) teach the method of changing a first password for securing files accessible by password data entry as defined in claim 18 wherein the

Art Unit: 2132

method of changing first password is automatically repeated at intervals (**see col.19-20 where it disclose the password particular to specific site (URL address (file) could be random for enhancing the security where such password corresponds to Applicant's first password as detailed in claim 11 above).**

10. **Claims 12, 13 and 20** are rejected under 35 U.S.C. 103(a) as being unpatentable over Nielson (6,182,229 B1) in view of Bellemore et al (6,145,086 A).

As per claim 12 Nielson (6,182,229 B1) teach all limitation of the claim but do not explicitly disclose the step of changing password includes: archiving the first password for use in accessing archival files secured with the first password. However Bellemore et al (6,145,086 A) disclose security and password mechanism with relationship to a database where the process of changing a password includes archiving the password as old password (**see col.5, lines 23-27 where it disclose history table contains used password as also depicted in fig.5, item 209**). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Bellemore et al's history table in Neilson's password database in order to archive old passwords for approval of new password and by comparison means to be sure the new password does not be the same as last N old passwords.

Art Unit: 2132

As per claim 13 Nielson (6,182,229 B1) teach all limitation of the claim but do not explicitly disclose the step of authorizing an individual requesting a change of the first password prior to changing the first password. However Bellemore et al (6,145,086 A) disclose the step of authorizing an individual requesting a change of the first password prior to changing the first password **(see col.6, lines 58-63 where the request for change of password is being done by client that corresponds to Applicant's individual)**. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Bellemore et al's history table and password change request in Neilson's password database security method in order to determine whether the proposed password may be used as a password by archive old passwords for approval of new password and by comparison means to be sure the new password does not be the same as last N old passwords.

As per claim 20 Nielson (6,182,229 B1) teach the method of changing first password is automatically repeated at intervals **(see col.19-20 where it disclose the password particular to specific site (URL address (file) could be random for enhancing the security where such password corresponds to Applicant's first password as detailed in claim 11 above)** but do not disclose explicitly changing the password is repeated upon detection of a breach of a password and upon expiry of a password. However Bellemore et al (6,145,086 A) disclose the method of automatically changing the password is repeated upon detection of a breach of a password and upon expiry of a password **(see fig.3, item 310, 314 and 318 where determination is made for**

Art Unit: 2132

breach of a password by monitoring the number of failed attempt; item 360, 370 and 328 in fig.3 represent the expiry of password monitoring). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Bellemore et al's history table and password change rules in Neilson's password database automatic password generation security method in order to invoke a security process in response to client transmission of a connection message to the database management.

Claim Rejections - 35 USC § 103

11. **Claim 14** is rejected under 35 U.S.C. 103(a) as being unpatentable over Nielson (6,182,229 B1) in view of Bellemore et al (6,145,086 A), and further in view of Brown et al (6,618,806 B1).

As per claim 14 Nielson (6,182,229 B1) in view of Bellemore teach all limitation of the claims applied to the claim 13 above but do not explicitly determining a user authorization method having an associated security level sufficient for accessing the secure password; authorizing an individual according to the secure authorization method. However Brown et al (6,618,806 B1) teach determining a user authorization method having an associated security level sufficient for accessing the secure password; authorizing an individual according to the secure authorization method **(see col.5, lines 5-29 where based on different set of instructions that corresponds to Applicant's associated security level a different biometric challenge being**

conducted that corresponds to Applicant's different methods and if verified the secure password is being retrieved for access); authorizing an individual according to the secure authorization method **(see col.5, lines 5-29 where based on the verification of biometric challenge authorization is being done by verification; col.8, lines 37-65 details the different authorization method or authentication).** It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Brown's biometric authorization methods that corresponds to different rules based on different instructions where the biometric information's are stored in the database in Nielson's password database automatic password generation security method in view of Bellemore et al's history table and password change rules in order to invoke a security process in response to client transmission of a connection message to the database management and to provide an authentication rule associated with a user based on different parameters of biometric data of a user.

Conclusion

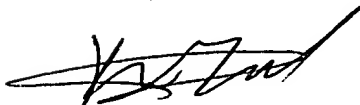
12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the

Art Unit: 2132

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (571) 272-3811. The examiner can normally be reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Kambiz Zand

11/28/2005

AU 2132